UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,849	11/04/2003	Thierry Le Pennec	243610US8X	5768

22850 7590 11/15/2007
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
RAMAKRISHNAIAH, MELUR	
ART UNIT	**PAPER NUMBER**
2614	
NOTIFICATION DATE	**DELIVERY MODE**
11/15/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/699,849	**Applicant(s)** LE PENNEC, THIERRY	
	Examiner Melur Ramakrishnaiah	**Art Unit** 2614	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 November 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-78* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-78* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *11-4-03,4-5-04,* 9-22-04

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1,6-7 15, 29, 38, are rejected under 35 U.S.C. 103(a) as being unpatentable over Deville et al. (INTEROPERABILITY ISSUES OF EXISTING COLLATERAL VIDEO TELECONFERENCE SYSTEMS AT THE UNITED STATES PACIFIC COMMAND, MILITARY COMMUNICATIONS CONFERENCE, 1994, MILCOM'94, Conference: Record, 1994 IEEE Fort Monmouth, N.J, U.S.A 2-5 Oct. 1994, New York, NY, USA, IEEE, US, XP010149676; hereinafter Deville) in view of Lauper et al. (US PAT: 6,717,607, hereinafter Lauper).

Regarding claim 1, Deville discloses a videoconferencing interface MCU device (first two paragraphs of abstract), comprising: at least three encryption devices (reads on multiple encryption devices) , each encryption device configured to encrypt with an encryption key ("encryption devices (key Generators", page 100 left-hand, column, second-to last paragraph), a secure interface connecting the at three encryption devices , and configured to relay video and audio traffic between the three encryption devices during a common video conferencing event. Deville further implies that videoconferencing device may be a multi-protocol interface device (this feature is implied by Deville by passages such as: This paper examines the issues of VTC systems interoperability and in specific examines [...] the lack of commonality of [...]

supporting equipment, page 97, second paragraph of abstract, "videoconferencing may cross between [...] network services, page 99, right-hand column, last 9 lines).

Deville differs from claim 1 in that he does not specifically teach: a) each encryption key is specified as a link interface encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol, b) a videoconferencing data buffer is specified, connected to secure interface and configured to buffer traffic relayed between the three encryption devices during a common videoconferencing event, c) is included a videoconferencing management device connected to secure interface and configured to hold ink-unique encryption keys.

However, Lauper discloses method and system for video conferences which teaches: participant image data and participant audio data are transmitted by the communication unit (20, fig. 1) to a central unit (30, fig. 1) . The transmission can take place, e.g. compressed and/or encrypted. The central unit (30, fig. 1), which receives and decompresses and/or decrypts the data. The transmission of data can take place, e.g., compressed and/or encrypted. The central unit (30, fig. 1) has a coding module (31, fig. 1, col. 5 lines 37-52) which clearly reads on) each encryption key is specified as a link interface encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol because the Lauper teaches each terminal uses a separate link to transmit encrypted audio and video to a central unit (30, fig. 1) where received audio and video from the terminals is decrypted and the central unit (30, fig. 1) transmits encrypted audio and video to the respective terminals. Further Lauper discloses: a videoconferencing data buffer is specified, connected to secure interface and configured to buffer traffic relayed between the three encryption devices during a common videoconferencing event (col. 6 lines 62-66). Lauper further implicitly teaches: a videoconferencing management device (30, fig. 1) connected to secure interface and configured to hold ink-unique encryption keys because the central unit decrypts and encrypts audio and video data which implies holding link unique encryption keys (col. 5 lines 30-52).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Deville's system to provide for the following: a) each encryption key is specified as a link interface encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol as this arrangement would provide the most obvious solution for assuring security of communication each separate link, b) a videoconferencing data buffer is specified, connected to secure interface and configured to buffer traffic relayed between the three encryption devices during a common videoconferencing event as this arrangement would facilitate processing data such as decryption and encryption by providing storage , c) is included a videoconferencing management device connected to secure interface and configured to hold ink-unique encryption keys as this arrangement would provide the most obvious solution to the necessarily arising problem of how the central unit can store and manage encryption keys for such decryption and re encryption.

Further claims 15, 29, 38, although drafted as separate independent claims, include all features of independent claim 1. The claims relate substantially the same subject matter as claim 1, but comprising more-encryption devices (four, rather than three as in claim 1), two interface engines (rather than one interface as in claim 1), two videoconference data buffers (rather than one as in claim 1), two videoconferencing management data archives (rather than one as in claim 1). Given the fact that multiplication or duplication of processing or storage means is well-known (for example, as a way of reducing the load on processing or storage means and improving the reliability of a system), the claims 15, 29, 38 are rejected on the same reasoning set forth in rejection of claim 1 above.

Deville differs from claims 6-7 in that he does not specifically teach: key management and synchronization device, encryption management and synchronization device.

However, Lauper teaches: key management (implied as he teaches encryption and decryption (col. 5 lines 37-49) and synchronization device (col. 5, line 65 – col. 6, line 2), encryption protocol management (col. 5 lines 37-49) and synchronization device (col. 5, line 65 – col. 6, line 2).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Deville's system to provide for the following: key management and synchronization device, encryption protocol management and synchronization device as this arrangement would provide necessary paraphernalia to carry out secure and satisfactory conferencing as shown by Lauper.

Claims 20-21 are rejected on the same basis as claims 6-7.

Claims 33-34 are rejected on the same basis as claims 6-7.

Claims 42-43 are rejected on the same basis as claims 6-7.

3. Claims 2, 5, 8 rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper as applied to claim 1 above, and further in view of Seamaan (US PAT: 5,680,392).

The combination differs from claim 2 in that it does not specifically teach data archive further configured to store at least one of: a management information, a session history, a diagnostic information, a session scheduling and billing information.

However, Seamaan discloses multimedia and multipoint telecommunications reservation systems which teach: storing management information, a session scheduling and billing information (abstract, col. 8 lines 31-50).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: data archive further configured to store at least one of: a management information, a session history, a diagnostic information, a session scheduling and billing information as this arrangement would provide required paraphernalia to conduct video conferences as taught by Seamaan.

Claim 5 is rejected on the same basis as claim 2.

Claim 8 is rejected on the same basis as claim 2.

Claim 16 is rejected on the same basis as claim 2.

Claim 19 is rejected on the same basis as claim 2.

Claim 22 is rejected on the same basis as claim 2.

Claim 32 is rejected on the same basis as claim 2.

Claim 35 is rejected on the same basis as claim 2.

Claim 41 is rejected on the same basis as claim 2.

Claim 44 is rejected on the same basis as claim 2.

4. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper as applied to claim 1 above, and further in view of Raike et al. (US PAT: 7,076,067, filed 7-10-2001, hereinafter Raike).

The combination differs from claim 3 in that it doers not specifically teach: secure interface device comprises a key management device.

However, Raike discloses encrypted key management which teaches: secure interface device (reads on server interface) comprises a key management device (fig. 1, abstract).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: secure interface device comprises a key management device as this arrangement would facilitate to mange information in a secure way as taught by Raike, thus managing information security.

Claim 17 is rejected on the same basis as claim 3.

Claim 30 is rejected on the same basis as claim 3.

Claim 39 is rejected on the same basis as claim 3.

5. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper as applied to claim 1 above, and further in view of Mulford (US PAT: 5,301,232).

The combination differs from claim 4 in that it does not specifically teach; secure interface comprises an encryption device programming device to enable one of local and remote encryption programming.

However, Mulford discloses method and apparatus for the over the air programming of communication devices which teach: secure interface comprises an encryption device programming device to enable one of local and remote encryption programming (abstract).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: secure interface comprises an encryption device programming device to enable one of local and remote encryption programming as this arrangement would facilitate update encryption information to the devices as taught by Mulford, thus providing most up to date encryption information.

Claim 18 is rejected on the same basis as claim 4.

Claim 31 is rejected on the same basis as claim 4.

Claim 40 is rejected on the same basis as claim 4.

6. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper as applied to claim 1 above, and further in view of Voois et al. (US PAT: 6,124,882, hereinafter Voois).

The combination differs from claim 9 in that he does not teach: secure interface comprises a videoconferencing diagnostic device.

However, Voois discloses videoconferencing apparatus and method therefor which teaches: secure interface comprises a videoconferencing diagnostic device (col. 15 lines 8-11).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: secure interface comprises a videoconferencing diagnostic device as this arrangement would facilitate to address equipment problems using diagnostic device as is well known in the art.

Claim 23 is rejected on the same basis as claim 9.

Claim 36 is rejected on the same basis as claim 9.

Claim 45 is rejected on the same basis as claim 9.

7. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper as applied to claim 1 above, and further in view of Boundy (US PAT: 6,981,022, filed 11-2-2001).

The combination differs from claim 10 in that it does not teach: secure interface comprises: a communication protocol translator configured to translate between at least link-unique communication protocols.

However, Boundy discloses using PSTN to convey participant IP addresses for multimedia conference which teaches: secure interface comprises: a communication protocol translator configured to translate between at least link-unique communication protocols (col. 2 lines 46-51).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: secure interface comprises: a communication protocol translator configured to translate between at least link-unique communication protocols as this arrangement would facilitate internetworking among devices using different protocols as taught by Boundy.

Claim 24 is rejected on the same basis as claim 10.

Claim 37 is rejected on the same basis as claim 10.

Claim 46 is rejected on the same basis as claim 10.

8. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper and Boundy as applied to claim 10 above, and further in view of Fernadez et al. (US PAT: 6,590,602, filed 12-21-2001, hereinafter Fernadez).

The combination differs from claim 11 in that it does not teach: a first of at least two link-unique communication protocols comprises one of H.320, H.323, H.324, and T.120, and a second of the at least two link-unique communication protocols comprises another .320, H.323, H.324, and T.120.

However, Fernandez discloses digital television with subscriber conference overlay which teaches: video conferencing signals transmitted or processed between receiver units comply with established video conferencing standards, such as H.320, H.323, H.324, and T.120 or other generally accepted industry video/data conferencing information (col. 3 lines 3-10).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: a first of at least two link-unique communication protocols comprises one of H.320, H.323, H.324, and T.120, and a second of the at least two link-unique communication protocols comprises another .320, H.323, H.324, and T.120 as this arrangement would provide well known industry standards for conducting video conference as taught by Fernandez.

Claim 25 is rejected on the same basis as claim 11.

9. Claims 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper as applied to claim 1 above, and further in view of Ragunathan et al. (US 2003/0142818A1, hereinafter Ragunathan).

The combination differs from claims 12-14 in that it does not specifically teach: link encryption protocols comprises one of: a manually provided encryption protocol, a DES protocol, a triple DES protocol, an AES protocol, and IDEA protocol, an automatic key exchange protocol, a manual key exchange protocol, a Diffe-Helman protocol, an RSA protocol.

However, Ragunathan discloses techniques for efficient security processing which teaches use of various encryption protocols such as DES, 3DES, AES and key exchange protocols such as RSA etc (paragraph: 0111).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: link encryption protocols comprises one of: a manually provided encryption protocol, a DES protocol, a triple DES protocol, an AES protocol, and IDEA protocol, an automatic key exchange protocol, a manual key exchange protocol, a Diffe-Helman protocol, an RSA protocol as this arrangement would provide required paraphernalia for secure transmission/reception of data as taught by Ragunathan.

Claims 26-28 are rejected on the same basis as claims 12-14.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 47 and 77 are rejected under 35 U.S.C 102(b) as being anticipated by Deville.

Regarding claim 77, Deville discloses a system for multi-protocol videoconferencing, comprising: means for receiving at an interface device a first set of encrypted video data from a first terminal over a first data communication link, means for decrypting the first set of video data at the interface device, and means for re-encrypting the relaying first set of data from the interface device to a second terminal over a second communication link, and a third terminal over a third communication link (page 100, left-hand column, first paragraph and page 100, right-hand column, second paragraph). Deville furthermore implies different communication protocols may be used for different links: the videoconferencing interface device may be multi-protocol interface device (this feature is implied by Deville by passages such as: "This paper examines the issues of VTC systems interoperability and in specific examines [...] the lack of commonality or standardization of [...] supporting VTC equipment" (page 97, second paragraph of abstract; "video conferencing may cross between [...] network services", page 99, right-hand column, last 9 lines).

Claim 47 is rejected on the same basis as claim 77.

12. Claims 48-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Nishizawa (JP408046723A).

Deville differs from claims 48-49 in that he does not specifically teach: communication protocol different from both the first and second communication protocols, communication protocol the same as one of first and second communication protocols.

However, Nishizawa discloses inter-communication system between video telephone sets of different kinds which teaches: communication protocol different from both the first and second communication protocols, communication protocol the same as one of first and second communication protocols (figs. 1-2, abstract).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify Deville's system to provide for the following: communication protocol different from both the first and second communication protocols, communication protocol the same as one of first and second communication protocols as this arrangement would facilitate communication between different type and/or same type of video terminals as taught by Nishizawa.

13. Claims 50-56, 60-67, 70-76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper.

Claims 50-56 recite the following: the step of decrypting the first set of video data comprises decrypting with a first encryption key and first encryption protocol, and the step of re-encrypting and sending the first set of video data to the second terminal comprises encrypting and a second set of protocol, the second encryption key different from the first encryption key and second encryption protocol different from the first encryption protocol, encrypting the first set of video with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as the first and second encryption protocols, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being the same as one of the first and second encryption keys and the third encryption protocol being same as a corresponding one of the first and second encryption protocols, the step of decrypting the first set of video data comprises decrypting with first encryption key and a first encryption protocol , and the step of re-encrypting the first set of video data to the second terminal comprises encrypting with a second encryption key and a second encryption protocol, the second encryption key different from the first encryption key and the first encryption protocol the same as the first encryption protocol, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols. Regarding these claims while Deville implicitly teach: the use of link-unique encryption key for each link, the key corresponding to common or link-unique encryption protocol (encryption devices are implicitly identified with key generators, see "encryption devices (Key Generators)", page 100, left hand column, second-to-last paragraph, and Key generators [...] are generally operated line pairs: page 100, left-hand column, second sentence of the last paragraph) and he also implies that different communication protocols may be used for different links (the video conferencing interface device may be multi-protocol interface device (this feature is implied by Deville by passages such as" "This paper examines the issues of VTC systems interoperability and in specific examines [...] the lack of commonality or standardization of [...] supporting VTC equipment, page 97, second paragraph of abstract: "video conferencing may cross between [...] network devices, page 99, right-hand column, last 9 lines), Lauper discloses video conferencing arrangement with remote terminals sending encrypted audio and video data to a a central unit (30, fig. 1), central unit receiving the encrypted audio and video data, decrypting the audio and video data and re-encrypting audio and video data and sending it to the different conference terminals (20, col. 5 line 30-52).

In light of these combined teachings, one of ordinary skill in the art at the time invention was made would have been able to arrive at the following: the step of decrypting the first set of video data comprises decrypting with a first encryption key and first encryption protocol, and the step of re-encrypting and sending the first set of video data to the second terminal comprises encrypting and a second set of protocol, the second encryption key different from the first encryption key and second encryption protocol different from the first encryption protocol, encrypting the first set of video with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as the first and second encryption protocols, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being the same as one of the first and second encryption keys and the third encryption protocol being same as a corresponding one of the first and second encryption protocols, the step of decrypting the first set of video data comprises decrypting with first encryption key and a first encryption protocol , and the step of re-encrypting the first set of video data to the second terminal comprises encrypting with a second encryption key and a second encryption protocol, the second encryption key different from the first encryption key and the first encryption protocol the same as the first encryption protocol, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting the first set of video data with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols in order to provide greater security to the data transmitted by each conference terminal to each other over separate communication links through a central unit.

Claims 57, 60-66, recite the following: receiving at the interface device a second set of encrypted video data from the second terminal over the second data communication link, decrypting the second set of video data at the interface device with second key unit and a second encryption protocol, and re-encrypting and relaying the second set of data from the interface device to the first terminal and the third terminal via third communication links, respectively, the step of decrypting the second set of video data comprises decrypting with a second encryption key and a second encryption protocol, and the step of re-encrypting and sending the second set of video data to the first terminal comprises encrypting with the first encryption key and first encryption protocol, the second encryption key different from the first encryption of key and the second encryption protocol different from the first encryption protocol, encrypting with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols, encrypting a third encryption key and a third encryption protocol, the third encryption key being the same as one of the first and second encryption keys and the third encryption protocol being the same as a corresponding one of the first and second encryption protocols, the step of re-encrypting and sending the second set of video data to the first terminal comprises encrypting with a first encryption key and a first encryption protocol, the second encryption key different from the first encryption key and second encryption protocol the same as the first encryption protocol, encrypting with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols.

Regarding these claims while Deville implicitly teach: the use of link-unique encryption key for each link, the key corresponding to common or link-unique encryption protocol (encryption devices are implicitly identified with key generators, see "encryption devices (Key Generators)", page 100, left hand column, second-to-last paragraph, and Key generators [...] are generally operated line pairs: page 100, left-hand column, second sentence of the last paragraph) and he also implies that different communication protocols may be used for different links (the video conferencing interface device may be multi-protocol interface device (this feature is implied by Deville by passages such as" "This paper examines the issues of VTC systems interoperability and in specific examines [...] the lack of commonality or standardization of [...] supporting VTC equipment, page 97, seconf paragraph of abstract: "video conferencing may cross between [...] network devices, page 99, right-hand column, last 9 lines), Lauper discloses video conferencing arrangement with remote terminals sending encrypted audio and video data to a a central unit (30, fig. 1), central unit receiving the encrypted audio and video data, decrypting the audio and video data and re-encrypting audio and video data and sending it to the different conference terminals (20, col. 5 line 30-52).

In light of these combined teachings, one of ordinary skill in the art at the time invention was made would have been able to arrive at the following: receiving at the interface device a second set of encrypted video data from the second terminal over the second data communication link, decrypting the second set of video data at the interface device with second key unit and a second encryption protocol, and re-encrypting and relaying the second set of data from the interface device to the first terminal and the third terminal via third communication links, respectively, the step of decrypting the second set of video data comprises decrypting with a second encryption key and a second encryption protocol, and the step of re-encrypting and sending the second set of video data to the first terminal comprises encrypting with the first encryption key and first encryption protocol, the second encryption key different from the first encryption of key and the second encryption protocol different from the first encryption protocol, encrypting with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols, encrypting a third encryption key and a third encryption protocol, the third encryption key being the same as one of the first and second encryption keys and the third encryption protocol being the same as a corresponding one of the first and second encryption protocols, the step of re-encrypting and sending the second set of video data to the first terminal comprises encrypting with a first encryption key and a first encryption protocol, the second encryption key different from the first encryption key and second encryption protocol the same as the first encryption protocol, encrypting with a third encryption key and a third encryption protocol, the third encryption key different from the first and second encryption keys and the third encryption protocol different from the first and second encryption protocols, encrypting with a third encryption key and a third encryption protocol, the third encryption key being different from the first and second encryption keys and the third encryption protocol being the same as one of the first and second encryption protocols in order to provide greater security to the data transmitted by each conference terminal to each other over separate communication links through a central unit.

Claims 67, 70-76, recite the following: receiving at the first interface device a third set of encrypted video data from a third terminal over the third data communication link, decrypting the third set of video data at the interface with a third encryption key and a third encryption protocol, and re-encrypting and relaying the third set of data from the interface device to the first and second terminals over the first and second communication links, the step of re-encrypting and sending the third set of video data to the first terminal comprises encrypting with a first encryption key and a first encryption protocol, the step of re-encrypting the third set of video data to the second terminal comprises encrypting with a second encryption key and a second encryption protocol, the second encryption key different from the first encryption key and the second encryption protocol different from the first encryption protocol, decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol different from the first and second encryption protocols, decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol the same as one of the first and second encryption protocols, decrypting with a third encryption key the same as one of the first and second encryption keys and a third encryption protocol the same as corresponding one of the first and second encryption protocols, the step of re-encrypting and sending the third set of video data to the first terminal comprises with a first encryption key and a first encryption protocol, the step of re-encrypting and sending the third set of video data to the second terminal comprises with a second encryption key different from the first encryption key and a second encryption protocol the same as the first encryption protocol, decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol different from the first and second encryption protocols, decrypting with a third encryption key different from the first and second encryption keys and a third encryption protocol the same as one of the first and second encryption protocols.

Regarding these claims while Deville implicitly teach: the use of link-unique encryption key for each link, the key corresponding to common or link-unique encryption protocol (encryption devices are implicitly identified with key generators, see "encryption devices (Key Generators)", page 100, left hand column, second-to-last paragraph, and Key generators [...] are generally operated line pairs: page 100, left-hand column, second sentence of the last paragraph) and he also implies that different communication protocols may be used for different links (the video conferencing interface device may be multi-protocol interface device (this feature is implied by Deville by passages such as" "This paper examines the issues of VTC systems interoperability and in specific examines [...] the lack of commonality or standardization of [...] supporting VTC equipment, page 97, seconf paragraph of abstract: "video conferencing may cross between [...] network devices, page 99, right-hand column, last 9 lines), Lauper discloses video conferencing arrangement with remote terminals sending encrypted audio and video data to a a central unit (30, fig. 1), central unit receiving the encrypted audio and video data, decrypting the audio and video data and re-encrypting audio and video data and sending it to the different conference terminals (20, col. 5 line 30-52).

In light of these combined teachings, one of ordinary skill in the art at the time invention was made would have been able to arrive at the following: receiving at the first interface device a third set of encrypted video data from a third terminal over the third data communication link, decrypting the third set of video data at the interface with a third encryption key and a third encryption protocol, and re-encrypting and relaying the third set of data from the interface device to the first and second terminals over the first and second communication links, the step of re-encrypting and sending the third set of video data to the first terminal comprises encrypting with a first encryption key and a first encryption protocol, the step of re-encrypting the third set of video data to the second terminal comprises encrypting with a second encryption key and a second encryption protocol, the second encryption key different from the first encryption key and the second encryption protocol different from the first encryption protocol, decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol different from the first and second encryption protocols, decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol the same as one of the first and second encryption protocols, decrypting with a third encryption key the same as one of the first and second encryption keys and a third encryption protocol the same as corresponding one of the first and second encryption protocols, the step of re-encrypting and sending the third set of video data to the first terminal comprises with a first encryption key and a first encryption protocol, the step of re-encrypting and sending the third set of video data to the second terminal comprises with a second encryption key different from the first encryption key and a second encryption protocol the same as the first encryption protocol, decrypting with a third encryption key different from the first and second encryption keys and with a third encryption protocol different from the first and second encryption protocols, decrypting with a third encryption key different from the first and second encryption keys and a third encryption protocol the same as one of the first and second encryption protocols in order to provide greater security to the data transmitted by each conference terminal to each other over separate communication links through a central unit.

14. Claims 58-59, 68-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Deville in view of Lauper as applied to claim 57 above, and further in view of Nishizawa (JP408046723A).

The combination differs from claims 58-59 in that he does not specifically teach: communication protocol different from both the first and second communication protocols, communication protocol the same as one of first and second communication protocols.

However, Nishizawa discloses inter-communication system between video telephone sets of different kinds which teaches: communication protocol different from both the first and second communication protocols, communication protocol the same as one of first and second communication protocols (figs. 1-2, abstract).

Thus, it would have been obvious to one of ordinary skill in the art at the time invention was made to modify the combination to provide for the following: communication protocol different from both the first and second communication protocols, communication protocol the same as one of first and second communication protocols as this arrangement would facilitate communication between different type and/or same type of video terminals as taught by Nishizawa.

Claims 68-69 are rejected on the same basis as claims 58-59.

Regarding claim 78, the combination of Deville in view of Lauper and Nishizawa teaches computer program product to store instructions corresponding to any one of the methods of claims 47-46 as set forth above.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Melur Ramakrishnaiah whose telephone number is (571)272-8098. The examiner can normally be reached on 9 Hr schedule.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Curt Kuntz can be reached on (571) 272-7499. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Melur Ramakrishnah

Melur Ramakrishnaiah
Primary Examiner
Art Unit 2614